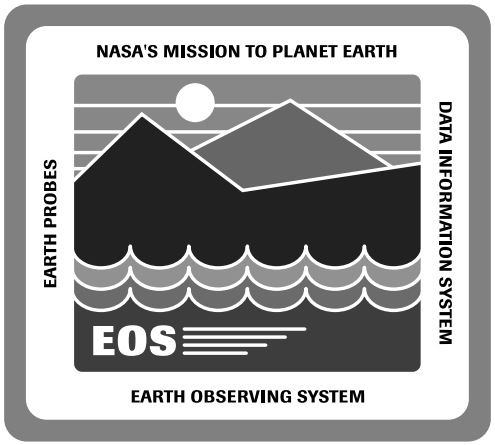


FOS Hardware Reliability/ Maintainability/Availability (RMA)

Modeling and Analysis

Bang Nguyen

18 October 1995

FOS CDR Roadmap

FOS Overview

FOS CDR Overview
- FOS CDR goals
- Driving requirements

Engineering Activities
- Activities since PDR
- FOS team approach

System Architecture
- Overview
- Features

FOS System Architecture

IST
- Capabilities
- Plans

Hardware Design
- Computers
- Peripherals

Network Design
- EOC LAN
- IST Connectivity

FOS Infrastructure
- Mgt Services
- Comm Services

Segment Scenarios
- End-to-End Flow
- Subsystem Interfaces
- Building block linkage

FOS System Design

Subsystem Design
- Detailed design
- FOS functions/tools
- Subsystem design features

RMA
- RMA allocation
- FMEA/CIL

FOT Operations

Operations Overview
- EOC facilities
- FOT positions

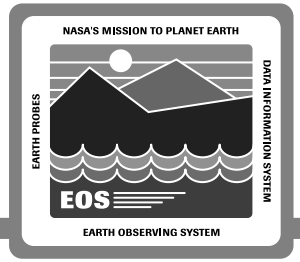
Operational Scenarios
- End-to-end flow
- Operations perspective
- FOT tool usage

Road to Launch

Development
- Release Plan
- Development approach

Testing
- Test approach
- Test organization

FOS Hardware RMA Agenda



RMA Analytical Assessment Approach

RMA COTS Data and Documentation Flow

RMA Measures

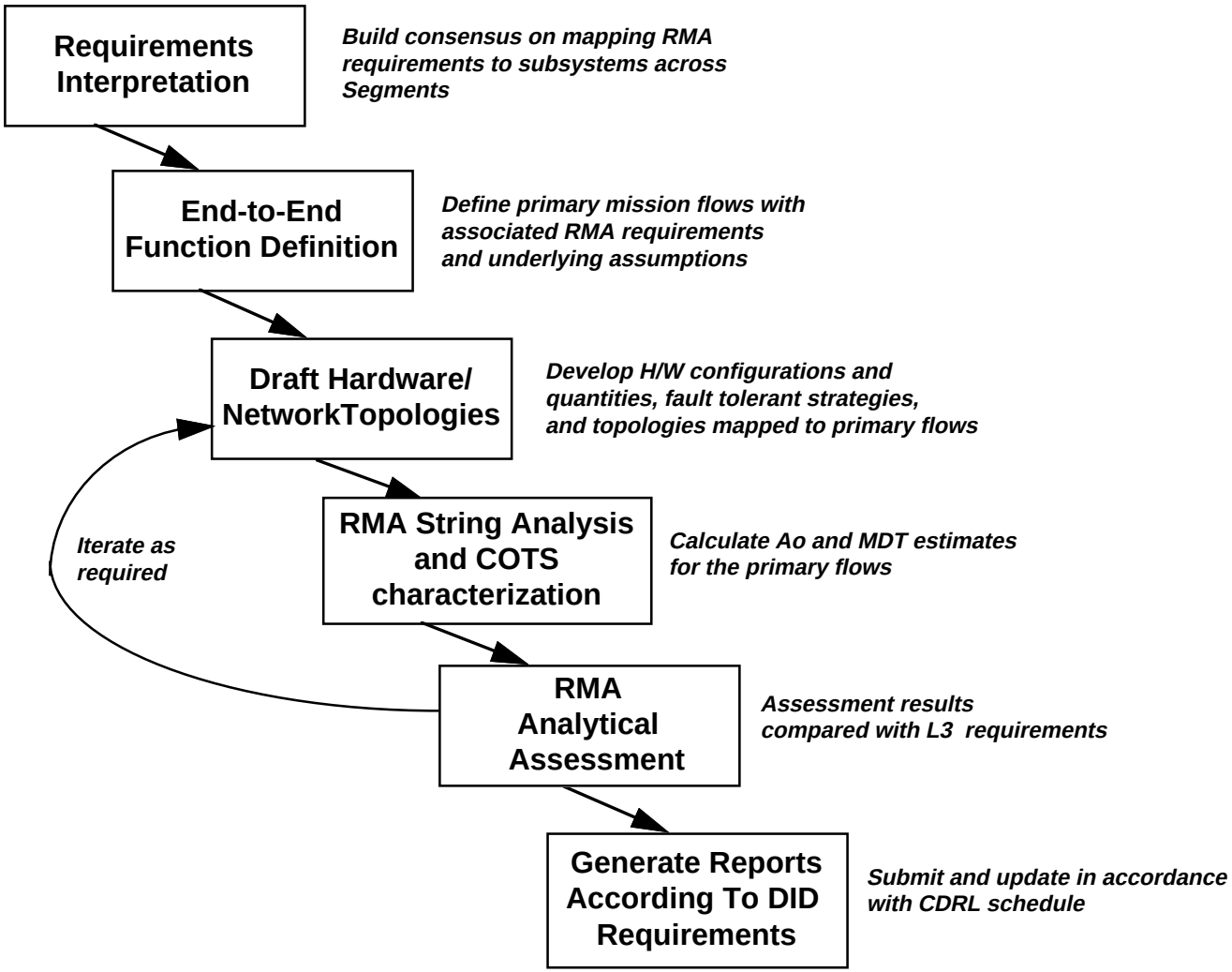
Availability Modeling Process

- **Assumptions**
- **Math models**
- **Block diagrams**
- **Availability results**

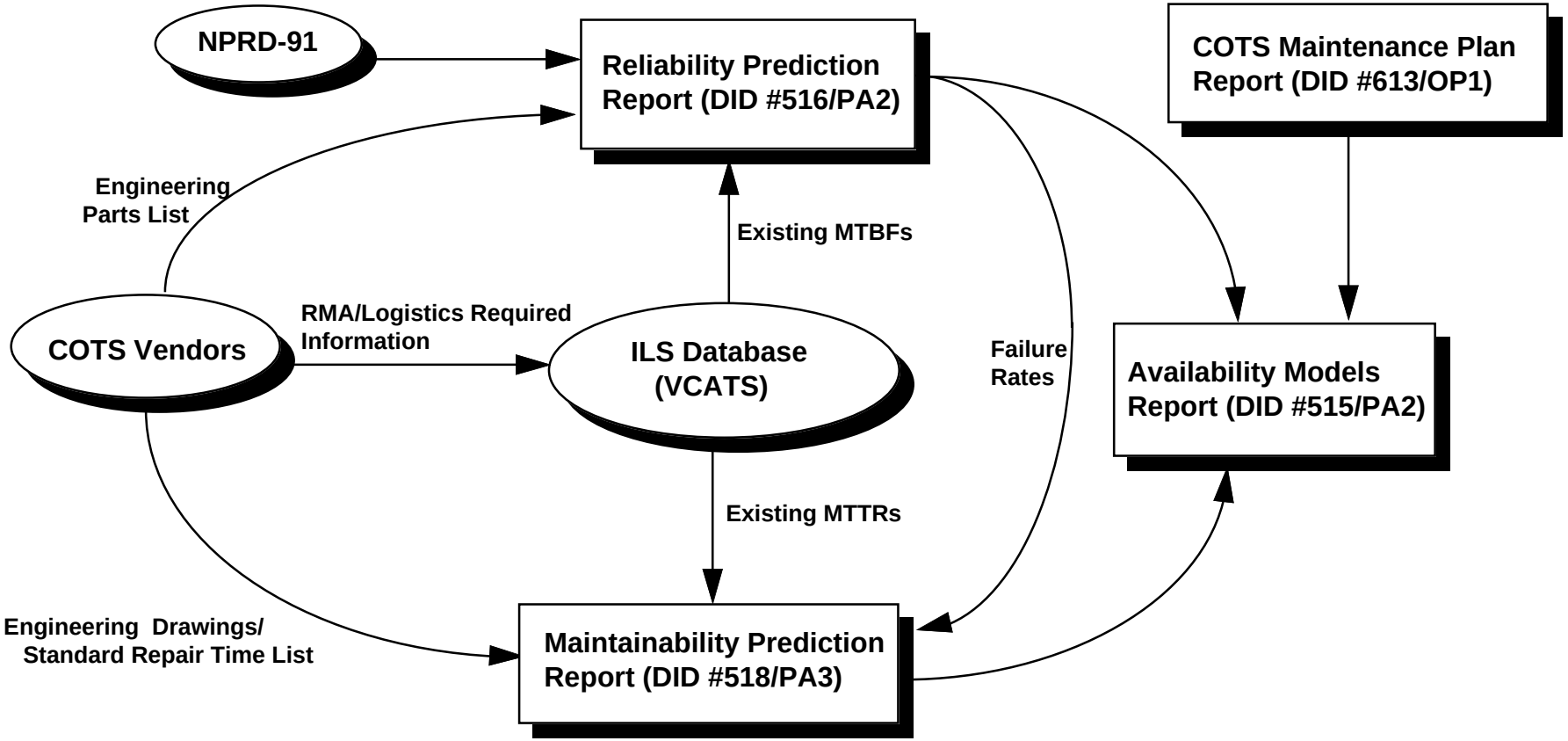
Failure Modes and Effects Analysis/Critical Items List (FMEA/CIL)

- **Requirements**
- **Assumptions and ground rules**
- **Failure criticality classification description**
- **Analysis results**

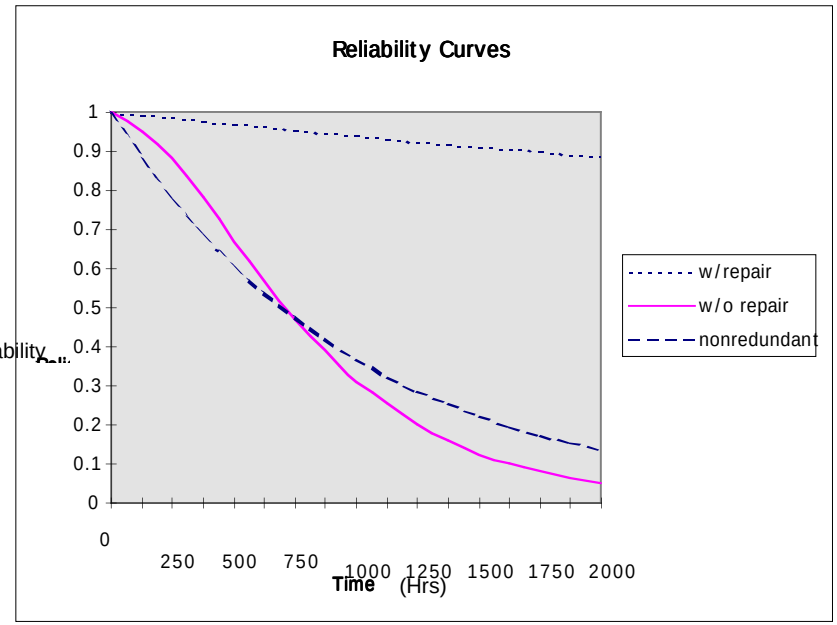
RMA Analytical Assessment Approach



RMA COTS Data and Documentation Flow



FOS RMA Measures



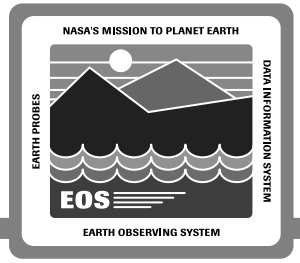
Hardware:

- **2 of 3 Warm standby redundant host servers**
- **RAID Level 5 with internal hot-swappable**
- **Redundant modules**
- **Dual FDDI networks with redundant concentrators and hubs**
- **Redundant hardware associated with critical real-time function**

Logistics:

- **On-line repair (ie. RAID, hot swappable modules)**
- **Sparing high failure rate LRUs at DAAC sites for quick turn around time**
- **Conducting self-maintenance where RMA requirements dictate**

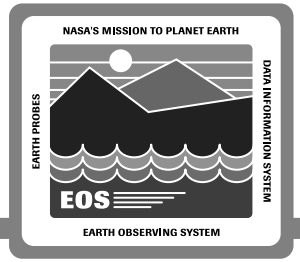
ECS Availability Modeling Assumptions



Assumptions Agreed To At PDR:

- **Availability calculations only apply to hardware configurations during staffed hours of operation**
- **EBNet-owned equipment is not part of the RMA calculations**
- **RMA data was based on COTS vendors and/or HAIS predictions**
- **Availability results were results were calculated using the reliability with repair model ror redundant system (the Einhorn equations)**
- **Software availability = 1.0 for analysis**
  - **Software and hardware will be measured during system test and operation**

ECS RMA Math Models



Operational Availability: $$Ao = \frac{MTBM}{MTBM + MDT}$$

Mean Time Between Maintenance (MTBM): $$\frac{1}{MTBM} = \frac{1}{MTBPM} + \frac{1}{MTBCM}$$

Mean Down Time (MDT): $MDT = MTTR + ALDT$

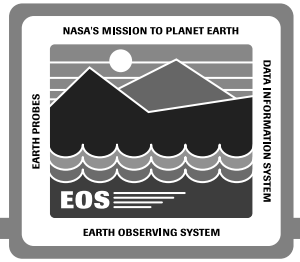
Mean Time To Repair (MTTR): $$MTTR = \frac{\sum_{i=1}^{i=n} \lambda i Mct_i}{\sum_{i=1}^{i=n} \lambda_i}$$

System with Active Off-Line Redundancies (Warm Standby):

$$MTBF_R = \frac{\mu + n(P+1)\lambda}{n[n\lambda + (1-P)\mu\lambda]}$$

$$\mu = \frac{1}{MDT + SwitchOverTin}$$

Math Models Abbreviations and Acronyms



Ao	Operational Avaliability
λ	Failure Rate Lambda in Failure Per Million Hours (FPMH)
λ **i**	Failure Rate Lambda in Failure Per Million Hours (FPMH) for the ith unit
$\mathbf{Mct_i}$	Mean Corrective Time for the ith Unit
MDT	Mean Down Time
MTBCM	Mean Time Between Corrective Maintenance
MTBF	Mean Time Between Failure
$\mathbf{MTBF_i}$	Mean Time Between Failure for the ith Unit
$\mathbf{MTBF_R}$	Mean Time Between Failure for Redundant Group
MTBM	Mean Time Between Maintenance
MTBPM	Mean Time Between Preventive Maintenance
MTTR	Mean Time To Repair
$\mathbf{MTTR_i}$	Mean Time To Repair for the ith Unit
$\mathbf{MTTR_R}$	Mean Time To Repair for Redundant Group
n	Total Number Of Units in the System
P	Probability of Switching from the Primary Unit To the Standby Unit
μ	Repair rate

FOS RMA Input Table

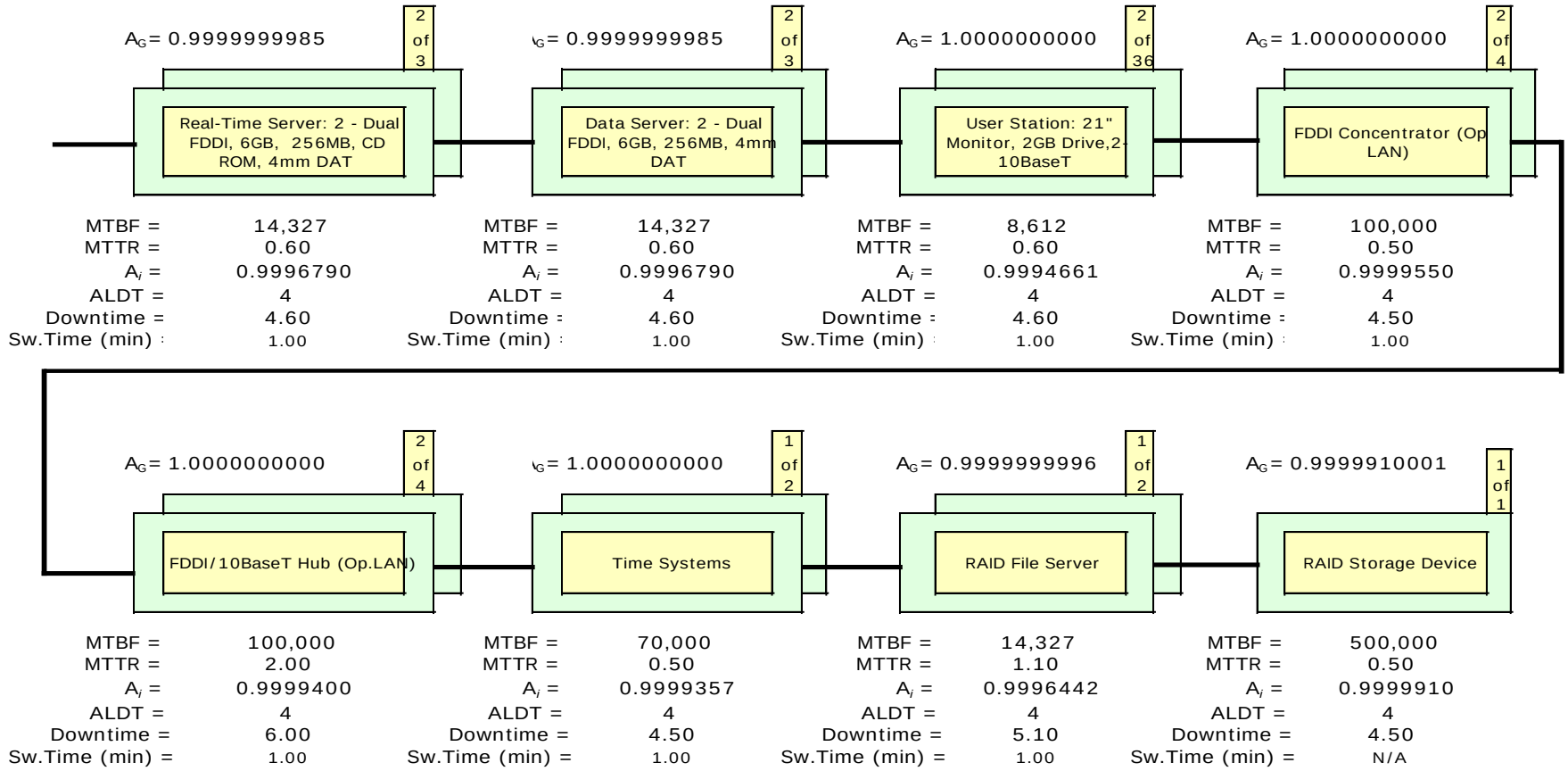
Equipment Description	Model/Part Number	MTBF (hour)	MTTR (hour)	Admin Logistics Delay Time (hour)	Switch over Time (min)	Total Down0time (hour)	# of Units Rqrd (m)	Total # Of Units (n)	Redundancy	Unit Availability (Ai)	P	Redundant Group Availability (m out of n)
Real-Time Server: 2-Dual FDDI, 6GB, 256MB, CD ROM, 4mm DAT	DEC Alpha 1000 4/233	14,327	0.60	4	1.0	4.60	2	3	standby off-line	0.9996790	1.0	0.999999998502
Data Server: 2 - Dual FDDI, 6GB, 256MB, 4mm DAT	DEC Alpha 1000 4/233	14,327	0.60	4	1.0	4.60	2	3	standby off-line	0.9996790	1.0	0.999999998502
User Station: 21" Monitor, 2GB Drive,2-10BaseT	SUN Sparc20 Model 71	8,612	0.60	4	1.0	4.60	2	36	standby off-line	0.9994661	1.0	1.000000000000
FDDI Concentrator (Op. LAN)	Synoptics 2914-04	100,000	0.50	4	1.0	4.50	2	4	standby off-line	0.9999550	1.0	1.000000000000
FDDI Concentrator (Support LAN)	Synoptics 2914-04	100,000	0.50	4	1.0	4.50	2	4	standby off-line	0.9999550	1.0	1.000000000000
FDDI/10BaseT Hub (Op.LAN)	Cabletron ESX-1320	100,000	2.00	4	1.0	6.00	2	4	standby off-line	0.9999400	1.0	1.000000000000
FDDI/10BaseT Hub (Support LAN)	Cabletron ESX-1320	100,000	2.00	4	1.0	6.00	2	4	standby off-line	0.9999400	1.0	1.000000000000
Time Systems	TYMESERV 2000IRIG	70,000	0.50	4	1.0	4.50	1	2	standby off-line	0.9999357	1.0	0.999999999985
RAID File Server	DEC Alpha 1000 4/233	14,327	1.10	4	1.0	5.10	1	2	standby off-line	0.9996442	1.0	0.999999999585
RAID Storage Device	Storage Works	500,000	0.50	4	N/A	4.50	1	1	Internal	0.9999910	1.0	0.999991000081
Multicast Server with Back-Up W/S	SUN Sparc20 Model 71	8,612	0.60	4	1.0	4.60	1	2	standby off-line	0.9994661	1.0	0.999999998964
Laser Printer	HP Laser Jet 4M	8,000	1.50	4	1.0	5.50	2	7	standby off-line	0.9993130	1.0	1.000000000000
Liner Printer	N/A	5,000	1.50	4	1.0	5.50	2	5	standby off-line	0.9989012	1.0	1.000000000000
Color Printer	HP Color Laser Jet	6,000	1.00	4	1.0	5.00	2	5	standby off-line	0.9991674	1.0	1.000000000000

FOS Critical R/T Ao = 0.9999909967
FOS Non-Critical R/T Ao = 0.9999909971

FOS Critical MDT (hrs) = 0.017
FOS Non-Crit. MDT (hrs)= 0.017

- **Light-Shaded Rows Are Critical Real-Time Items**

Sample Of An RMA String:
FOS Critical Real-Time Functions (EOSD3800)

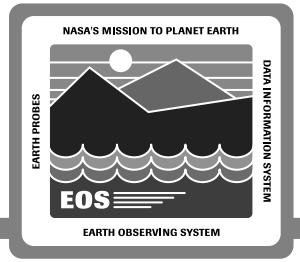


FOS RMA Results

No Single Point Of Failure Requirement Allows FOS Architecture To Meet All Quantitative RMA Requirements With Considerable Margin

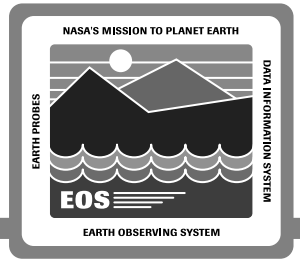
	Specification Requirements		Analytical Results	
	Ao	MDT	Ao	MDT
Critical R/T (EOSD3800)	0.99980 (Total Down Time of 1.75 hrs per year)	1 min.	0.9999909971 (Total Down Time of 5.0 min per year)	1 min.
Non-Critical R/T (EOSD3810)	0.99250 (Total Down Time of 6.58 hrs per year)	5 min.	0.9999909967 (Total Down Time of 5.0 min per year)	1 min.

FMEA/CIL Requirements: FOS Critical Real-Time Systems



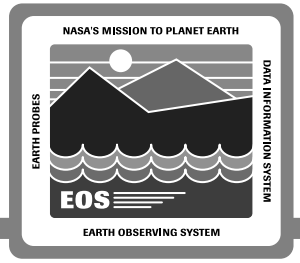
- **In Accordance With GSFC S-302-89-01 Guidelines**
- **Bottom- Up Analysis From Equipment/LRU Level**
- **To ensure:**
  - **1- No Single Failure Will Adversely Affect The Performance Of The Redundant Capability**
  - **2- No Single Failure Will Prevent The Successful Removal Of Power From A Failed Flight Instrument**
  - **3- No Single Point Of Failure In The Component That Provides Critical Real-Time Functions**

FOS FMEA Assumptions and Ground Rules



- **Only one failure mode exists at a time**
- **Failure modes are defined per the GSFC S-302-89-01, Procedures for Performing a FMEA:**
  - **Premature operation**
  - **Failure to operate at a prescribed time**
  - **Failure to cease operations when required**
  - **Failure during operation**
- **Failures due to human error in system setup (e.g., procedural or induced errors) were not considered. Such items were considered in the Hazard Analysis, DID 513/PA2**

Failure Mode Criticality Classifications



Failure Mode Criticality Classifications are Defined and Assigned With Number in Accordance With Paragraph 5.3.4 of the ECS Performance Assurance Requirements (PAR) as Follows:

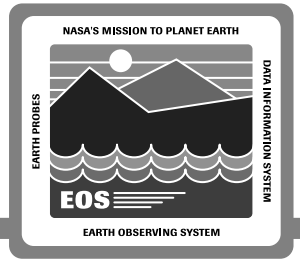
Criticality 1: A single failure that could result in loss of human life, serious injury personnel, loss of mission, or loss of spacecraft and instrument or a major portion of the ECS facility.

Criticality 2: A single failure that could result in a loss of a primary mission objective (as defined by the ECS project) or significant damage to the spacecraft and instrument.

Criticality 3: A single failure that could result in a loss of a secondary mission objective (as defined by the ECS project), significant damage to an instrument or degradation of science products (as defined by the ECS project), or loss of data identified as critical by the Project.

Criticality 4: Loss of system capability that does not significantly impact the science mission.

FOS FMEA Results



Analysis Documented In Accordance With DID 517/PA2:

- **34 Unique LRUs analyzed**
- **123 Failure Modes identified**
- **All Failure Modes are criticality 4 classifications**
- **No Failure Modes with criticality 1, 2, or 3 identified**
- **No single point of failure identified**